03CO 0420 #3

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
028420-0012CIP

In Re Application Of: P. Kocher et al.

Serial No.	Filing Date	Examiner	Group Art Unit
10/005,105	December 3, 2001	Unassigned	Unassigned

Title: Differential Power Analysis Method and Apparatus

Address to:
Assistant Commissioner for Patents
Washington, D.C. 20231

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

37 CFR 1.97(c)

2. □ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), provided that the Information Disclosure Statement is filed before the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

   □ the statement specified in 37 CFR 1.97(e);

   OR

   □ the fee set forth in 37 CFR 1.17(p).

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT
(Under 37 CFR 1.97(b) or 1.97(c))

Docket No.
028420-0012CIP

In Re Application: **P. Kocher et al.**

Serial No.	Filing Date	Examiner	Group Art Unit
10/005,105	December 3, 2001	Unassigned	Unassigned

Differential Power Analysis Method and Apparatus

Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

□ A check in the amount of is attached.

☒ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. 19-2385 as described below. A duplicate copy of this sheet is enclosed.

- □ Charge the amount of
- □ Credit any overpayment.
- ☒ Charge any additional fee required.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (F

(Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited Jan. 16, 2002 with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Jan Steele

Signature of Person Mailing Correspondence

Jan Steele

Typed or Printed Name of Person Mailing Certificate

***This certificate may only be used if paying by deposit account.**

Signature

Dated: **January 16, 2002**

Joseph Yang, Ph.D.
Registration No. 41,387
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570

cc:

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

ATTY DOCKET NO. 028420-0012CIP	SERIAL NO. 10/005,105
P. Kocher et al.	
FILING December 3, 2001	GROUP Unassigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		4,200,770	4/1980	Hellman et al.	178	22	
		4,405,829	9/1983	Rivest et al.	178	22.1	
		4,759,063	7/1988	Chaum	380	30	
		4,799,258	1/1989	Davies	380	21	
		4,905,176	2/1990	Schulz	364	717	
		4,908,038	3/1990	Matsumura et al.	902	5	
		5,136,646	8/1992	Haber et al.	380	49	
		5,297,207	3/1994	Degele	380	46	
		5,401,950	3/1995	Yoshida	235	487	
		5,404,402	4/1995	Sprunk	380	4	
		5,539,827	07/1996	Liu	380	37	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

			"Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, U.S. Department of Commerce, National Institute of Standards and Technology, January 1994, pp. 1-53.
			RSA Data Security, RSAREF Cryptographic Toolkit Source Code, File R_RANDOM.C, available from ftp://ftp.rsa.com, created 1991, pp. 1-2.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. 028420-0012CIP	SERIAL NO. 10/005,105
	P. Kocher et al.	
	FILING December 3, 2001	GROUP Unassigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		5,546,463	8/1996	Caputo et al.	380	25	
		5,663,896	9/1997	Aucsmith	395	187.01	
		5,664,017	9/1997	Gressel et al.	380	30	
		5,727,063	3/1998	Aiello et al.	380	46	
		5,778,074	7/1998	Garcken et al.	380	37	
		5,812,669	9/1998	Jenkins et al.	380	25	
		5,835,599	11/1998	Buer	380	29	
		5,838,795	11/1998	Mittenthal	380	28	
		5,848,159	12/1998	Collins et al.	380	30	
		5,991,415	11/1999	Shamir	380	30	
		6,041,122	03/2000	Graunke et al.	380	21	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

			M. Bellare et al., "Incremental Cryptography: The Case of Hashing and Signing" in: Desmedt, Y., Advances in Cryptology - Crypto 94 Proceedings (Springer-Verlag, 1994) pp. 216-233.
			Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in: Koblitz, N., Advances in Cryptology - Crypto '96 (Berlin, Springer, 1996), pp. 104-113.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	ATTY DOCKET NO. 028420-0012CIP	SERIAL NO. 10/005,105
	P. Kocher et al.	
	FILING December 3, 2001	GROUP Unassigned

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		6,041,412	3/2000	Timson, et al.	713	200	
		6,049,613	4/2000	Jakobsson	380	47	
		6,064,724	5/2000	Kelly	379	92.04	
		6,064,740	5/2000	Curiger et al.	380	265	
		6,069,954	5/2000	Moreau	380	28	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

			Schneier, Bruce, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, Inc. 10/18/95, pp. 34-41, 390-392 and 480-481.
			Krawczyk, H., et al., "HMAC: Keyed-Hashing for Message Authentication," Network Working Group Request for Comments RFC 2104, February 1997, pp. 1-11.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 028420-0012CIP	Application Number 10/005,105
	Applicant(s) P. Kocher et al.	
	Filing Date December 3, 2001	Group Art Unit Unassigned

*EXAMINER INITIAL		OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*
		Ryan, J. "Blinds for Thermodynamic Cipher Attacks," unpublished material on the World Wide Web at http://www.cybertrace.com/thrmatak.html, March 1996, pp. 1-7.
		"Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, December 30, 1993, pp. 1-21.
		Biham, E., et al., "Differential Fault Analysis of Secret Key Cryptosystems," in: Kaliski, B., Advances in Cryptology-CRYPTO '97 (Berlin, Springer, 1997), 17th Annual International Cryptology Conference, August 17-21, 1997, pp. 513-525.
		Based on "Karn/Hoey/Outerbridge" implementation (KHODES): "File DESC.C from RSAREF - Data Encryption Standard routines for RSAREF."
		Alfred J. Menezes et al., "Handbook of Applied Cryptography" (CRC Press, 1996), pages including 285-298, 312-319, 452-462, 475, 515-524.
		Bank Technology News. Cries of Wolf Over Smart Card Security? Faulkner & Gray, Inc. 01 November 1996.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.